

Rapport : analyse du marché des MSP et attentes des clients

kaspersky

Table des matières

Introduction 3
Principales conclusions 5
Méthodologie 6
Services informatiques externalisés : changer la dynamique du marché des MSP 7
Les perspectives européennes 7
Quel est le moteur de la décision ? 8
Le paysage européen du marché des MSP : priorités et difficultés 11
Un MSP « typique » 11
Aspects positifs et négatifs 12
Le partenaire de sécurité idéal 13
Les hauts et les bas d'une relation 15
Qualités et difficultés 15
Impact sur les MSP 16
Conclusion et recommandations 17

Introduction

Le marché des fournisseurs de services managés (MSP) représente une immense activité. Ce qui n'était à la base qu'un rôle de revendeur informatique, visant à fournir, installer et gérer une application spécifique, a évolué vers un statut de MSP, devenant partie intégrante de l'approvisionnement informatique et du réseau de support d'une entreprise. Pour de nombreuses entreprises, un MSP est une extension de leur équipe informatique, ou, dans certains cas, leur équipe informatique tout entière. Il comble souvent les manques en matière de compétences et de ressources en interne, pour s'assurer que les opérations informatiques se déroulent sans heurts et avec succès.

Les PME, en particulier, comptent sur les MSP en tant que conseiller de confiance tandis que l'environnement informatique évolue. De plus, les compétences et les budgets internes restreignent souvent la capacité des PME à suivre ces évolutions. La croissance continue et prévue dans les services Cloud n'est qu'un exemple de cas où les MSP jouent un rôle important en aidant les petites entreprises à profiter des applications basées dans le Cloud.

Gartner prédit que le marché mondial des services de Cloud public augmentera de 17,5 % en 2019 pour constituer un total de 214,3 milliards de dollars, offrant une grande opportunité aux MSP qui pourront ainsi aider les entreprises à réussir ces projets. En effet, jusqu'en 2022, Gartner prévoit que la taille et la croissance du marché des services Cloud représenteront près de trois fois la croissance de l'ensemble des services informatiques.

Il n'est donc pas surprenant que, selon des chiffres récents, le marché des services managés devrait passer de 180,5 milliards de dollars à 282 milliards de dollars d'ici 2023. Cela est en grande partie dû aux sociétés qui s'appuient sur les MSP pour « stimuler la productivité de leur entreprise et [répondre] aux demandes croissantes de services managés basés dans le Cloud ». Une autre raison de cette augmentation est la valeur associée à l'externalisation de la gestion de l'informatique et de la sécurité.

Force est de constater que les cyberattaques malveillantes ciblant les entreprises sont à la hausse, ce qui rend ces dernières beaucoup plus conscientes des risques et des conséquences d'une violation de données ou d'une attaque de ransomware sur leur activité. Alors que de nombreux cas connus par le public portent sur de grandes sociétés qui subissent une violation de données, les petites entreprises et celles de la chaîne d'approvisionnement sont tout aussi vulnérables et les conséquences tout aussi graves.

La technologie étant l'épine dorsale de toute entreprise (quelle que soit sa taille ou son secteur), il peut être difficile de suivre le rythme auquel apparaissent les applications novatrices et les menaces de sécurité. Cela est particulièrement vrai pour les sociétés manquant de budget ou de ressources à leur échelle. En fait, de récentes recherches de Kaspersky ont permis de constater que les entreprises de moins de 500 salariés sont plus susceptibles de faire appel à des fournisseurs de services externalisés, afin de garantir une gestion et une sécurité performantes de leurs infrastructures informatiques. 40 % des entreprises externalisent leur gestion informatique et 33 % externalisent spécifiquement leur sécurité informatique à un tiers.

Ces chiffres élevés suggèrent qu'avec des budgets et des ressources restreints, les entreprises considèrent que la meilleure solution est de demander de l'aide à un expert externe. Bien que cela constitue une énorme opportunité pour les MSP (attestée par la croissance prévue du marché mondial), cette situation présente aussi des difficultés et crée d'énormes attentes à l'égard des prestataires, pour combler les manques de compétences, ainsi qu'assumer la responsabilité en cas de violation ou d'interruption de ses activités.

Afin de comprendre les difficultés et les opportunités actuelles pour les MSP dans toute l'Europe, ce rapport examine la dynamique du marché en évolution, ainsi que l'impact du changement des relations avec le client et les attentes de ce dernier dans le secteur des MSP. Il fournit également des recommandations dédiées aux MSP, pour leur permettre de tirer parti des opportunités et de maintenir des relations à long terme avec leurs clients, quels que soient les obstacles qui entravent leur chemin.

Principales conclusions

- L'externalisation des services informatiques, et en particulier de la sécurité, est à la hausse. Un tiers (33 %) des entreprises de moins de 500 salariés en Europe externalisent actuellement la gestion de leur sécurité informatique et 21 % prévoient de le faire au cours des 12 prochains mois.
- La tendance à externaliser est stimulée en grande partie par l'absence de compétences internes et par le souhait des entreprises de tirer le meilleur parti des budgets informatiques disponibles. La moitié (51 %) des entreprises externalisent pour compléter des compétences internes et 52 % estiment que travailler de cette manière les aidera à réduire les coûts liés à la sécurité.
- Lorsque les budgets informatiques sont réduits, les entreprises s'orientent vers l'externalisation comme la façon la plus rentable de garantir une qualité de services et de répondre aux futurs besoins en gestion de la sécurité informatique.
- Trois quarts (75 %) des MSP admettent que satisfaire les demandes des clients est un défi majeur, les deux tiers (68 %) d'entre eux rencontrant des difficultés pour maintenir la rentabilité dans leurs relations clients en raison d'une attribution de ressources excessive pour traiter les problèmes de sécurité axés sur l'utilisateur.
- La réputation du marché est essentielle pour attirer et garder des clients, 83 % des MSP s'appuyant sur le bouche à oreille, les recommandations, les fournisseurs abordant directement des clients potentiels (50 %) et le parrainage d'événements (48 %), afin d'accroître leur clientèle.
- Il en va de même lorsque les MSP doivent choisir un partenaire de sécurité : 92 % prennent leur décision en fonction de la réputation et du prix. Comme avec leurs propres clients, afin d'ajouter de la valeur à leur offre, les MSP doivent travailler avec un partenaire qui a non seulement les solutions et l'expertise appropriées pour les aider, mais qui peut aussi fournir ces services au meilleur prix.
- Concernant les attentes des MSP d'aujourd'hui, être un expert en Cloud et en infrastructure sur site est la principale qualité dont les clients ont besoin (84 %). Les capacités en cybersécurité se situent également en haut de la liste, 74 % des clients les considérant comme un atout clé chez leur partenaire MSP.
- Faire face à l'imprévu peut mettre à rude épreuve les relations clients et peut avoir un impact financier pour les MSP, ce qui rend plus difficile le maintien de la croissance du chiffre d'affaires. Trois quarts (78 %) des clients s'attendent à ce que les MSP traitent des problèmes en dehors de leur contrat et 65 % des MSP résolvent des problèmes de sécurité provenant d'erreurs de l'utilisateur plutôt que liés aux services qu'ils gèrent.
- Par conséquent, les MSP assument souvent la responsabilité pour des incidents de sécurité qui ne sont pas le résultat de leur négligence. 43 % des entreprises qui ont subi une violation de données ont blâmé leurs MSP, 27 % l'imputant à un manque de connaissances en matière de sécurité informatique de la part de leur fournisseur de services.

Méthodologie

Les résultats présentés dans ce rapport sont tirés de deux sources de données :

- Des entretiens téléphoniques menés en juillet et en août 2019 auprès de 101 salariés de MSP au Royaume-Uni, en France, en Allemagne, en Espagne, en Italie, en Autriche, en Suède et au Danemark.
- L'enquête 2019 de Kaspersky sur les risques liés à la sécurité informatique pour les entreprises : un sondage annuel en ligne auprès de décideurs informatiques d'entreprises, mené en juin 2019 dans 23 pays. Ce rapport se concentre sur les réponses de personnes travaillant dans des entreprises en Europe, qui comptent moins de 500 salariés.

Services informatiques externalisés : changer la dynamique du marché des MSP

Les perspectives européennes

Le rôle d'un MSP pour les entreprises est en train de changer, passant du rang de simple fournisseur de solutions à celui de conseiller de confiance et pilier pour la réussite des opérations. L'externalisation des services informatiques devient ainsi la nouvelle norme, car les entreprises se tournent vers des experts qui peuvent donner des conseils et gérer leur infrastructure informatique tentaculaire, ainsi que tout ce qui l'accompagne.

40 % des entreprises en Europe comptant moins de 500 salariés externalisent actuellement la gestion de leur service informatique à un tiers. Un tiers (33 %) d'entre elles externalisent également leur gestion de la sécurité informatique, révélant ainsi qu'il s'agit d'un domaine clé du support informatique, dont les entreprises délèguent désormais la responsabilité à leur fournisseur.

Il s'agit d'un thème commun dans toute l'Europe, les Pays-Bas ouvrant la marche concernant l'externalisation des service de sécurité informatique (45 %), suivis de près par la Suède (39 %) et l'Italie (39 %). D'autres pays accélèrent cependant le pas : il est prévu que la Pologne (35 %), la République tchèque (24 %), la France (22 %) et l'Espagne (22 %) affichent la plus forte croissance en matière d'externalisation de gestion de la sécurité informatique au cours des 12 prochains mois.

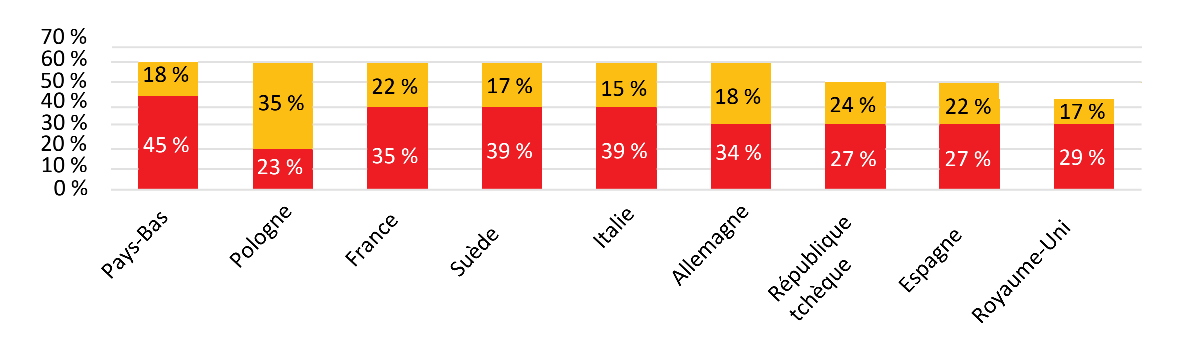


Figure 1. Niveaux actuels et croissance prévue en matière d'externalisation de la sécurité informatique au cours des 12 prochains mois

Pour les entreprises qui adoptent une approche d'externalisation, le modèle d'engagement peut prendre différentes formes, selon leurs exigences spécifiques. Pour la plupart des MSP, les clients souhaitent un partenariat ou une approche mixte (51 %), complétant leurs compétences internes avec une expertise externe pour obtenir un équilibre parfait dans la gestion de la sécurité informatique. Cependant, près d'un tiers (29 %) des MSP estiment que les entreprises préfèrent leur confier la totalité de la fonction informatique, y compris la sécurité informatique.

Quel est le moteur de leur décision ?

Comme pour de nombreuses décisions, le coût est le critère principal, derrière la nécessité d'externaliser la gestion de la sécurité informatique. Plus de la moitié des sociétés qui envisagent d'externaliser la gestion de la sécurité informatique (52 %) estiment que travailler de cette manière les aidera à réduire les coûts liés à la sécurité. Plus d'un tiers (38 %) cherchent ainsi à externaliser tout le service informatique à une tierce partie, notamment la sécurité. Il est intéressant de signaler qu'un tiers (33 %) des sociétés considèrent l'externalisation de la sécurité informatique comme un moyen de respecter l'accord de service et de déléguer la responsabilité. La même proportion d'entreprises (32 %) reconnaît qu'elle ne dispose tout simplement pas des ressources internes ou de l'expertise nécessaires pour fournir les niveaux de sécurité requis pour ses activités.

Cependant, il existe des raisons pour lesquelles les entreprises choisissent de ne pas externaliser leur sécurité informatique, ce que les MSP doivent garder à l'esprit, car ils cherchent à augmenter leurs offres et à établir des relations durables avec les clients. Bien que les compétences soient souvent citées comme la raison principale de travailler avec une tierce partie, 40 % des entreprises avec lesquelles nous avons parlé sont contre l'externalisation de la gestion de la sécurité informatique, et pensent qu'elles possèdent suffisamment d'expertise en interne pour gérer leur propre sécurité informatique. Un autre sujet de préoccupation pour un tiers des entreprises (33 %) est la perception des coûts élevés associés à l'externalisation de leur gestion de la sécurité informatique.

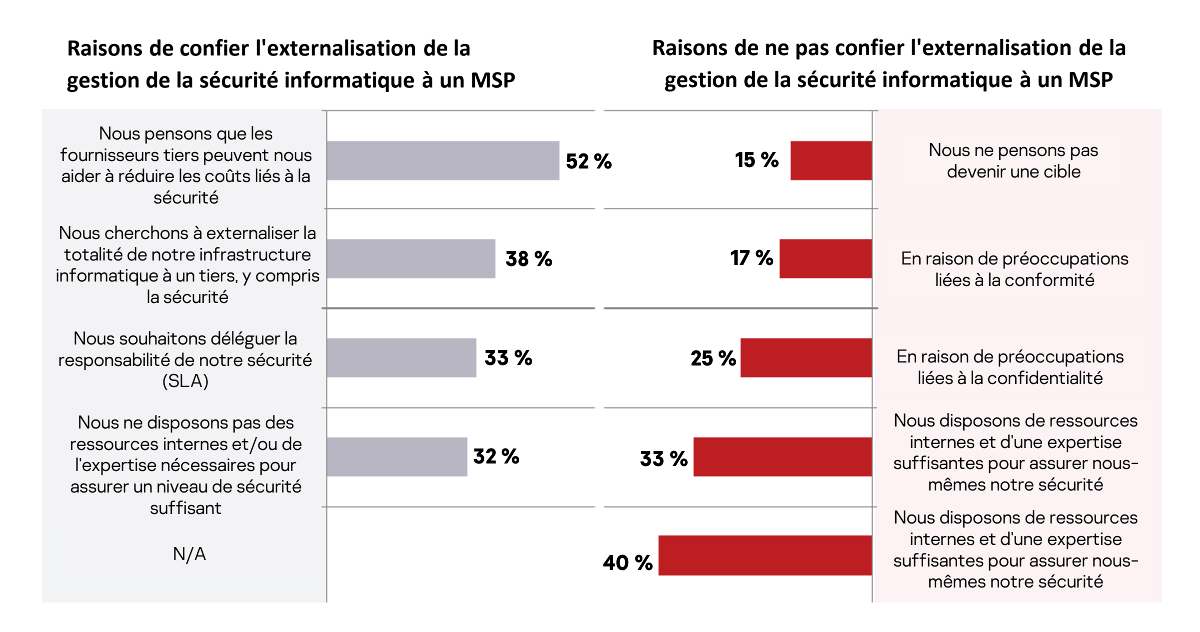


Schéma 2. Avantages et inconvénients de l'externalisation de la gestion de la sécurité informatique auprès d'un MSP

Une recherche plus poussée sur le processus de prise de décision au sein de différents secteurs indique qu'il existe divers facteurs poussant à l’externalisation. Alors que les économies de coûts sont le moteur pour la plupart des secteurs, le domaine de la santé cite la protection de la vie privée comme principale raison de ne pas externaliser et le secteur de l'éducation estime que le prix des solutions tierces est trop élevé.

Le dilemme du coût par rapport au budget est certainement une difficulté que les MSP et les entreprises doivent attaquer de front. Fait intéressant, les entreprises qui s'attendent à ce que leurs budgets de sécurité informatique augmentent préfèrent renforcer le personnel interne spécialisé en informatique. Toutefois, une diminution de budget poussera les entreprises à s'orienter vers un MSP pour accompagner la future gestion de leur sécurité informatique, ce qui sous-entend qu'elles estiment plus avantageux de travailler ainsi lorsque les budgets sont restreints.

Comment le changement des budgets dédiés à la sécurité informatique a-t-il un impact sur la future gestion de la sécurité ?

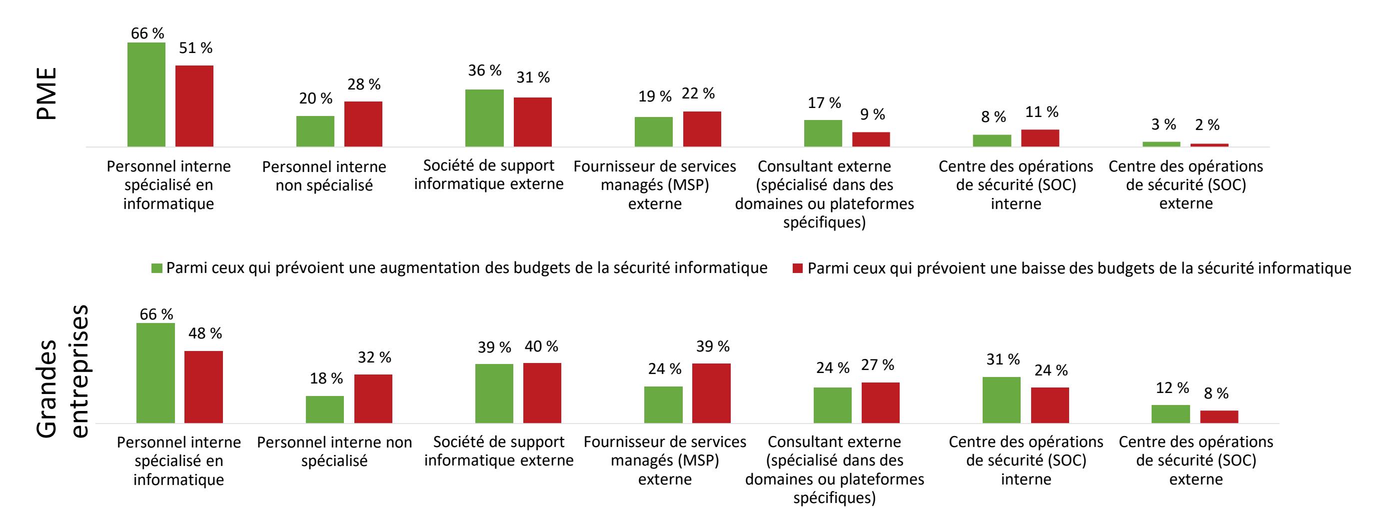


Schéma 3. Comment le changement des budgets dédiés à la sécurité informatique a-t-il un impact sur la future gestion de la sécurité ?

Il est évident que le fait de tirer le maximum des budgets disponibles et de garantir que les ressources et les protections appropriées sont en place stimule la croissance commerciale des MSP. Cependant, les mêmes moteurs peuvent aussi dissuader beaucoup d'entreprises et de secteurs potentiels d'investir dans l'assistance externe.

L'environnement européen des MSP : priorités et difficultés

Un MSP « typique »

Nous avons déjà établi que le rôle et les responsabilités du MSP sont en train de changer. Il est donc logique de redéfinir la situation de la plupart des MSP dans le contexte actuel, afin d'évaluer les opportunités et les difficultés spécifiques qu'ils rencontrent.

La majorité (57 %) des MSP à qui nous avons parlé ont entre deux et 20 salariés et en dépit d'être de petites entreprises, un tiers (32 %) d'entre eux s'occupent de clients comptant plus de 300 salariés. 50 % des MSP travaillent avec un vaste éventail de clients dans divers secteurs, dont un tiers (35 %) se concentre principalement au soutien des PME.

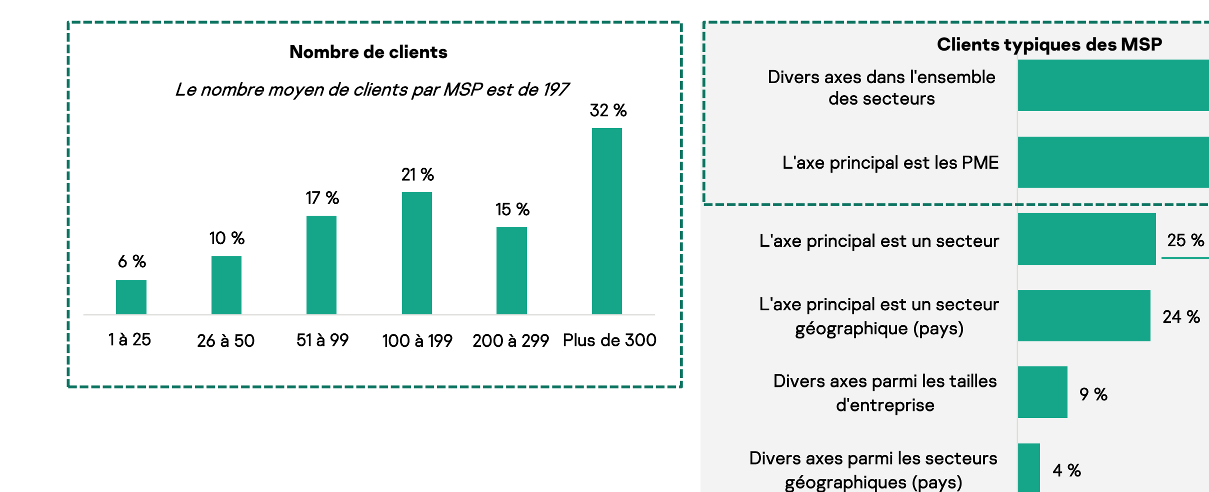


Figure 4. Nombre de clients de MSP et clients typiques de MSP

Une base de clients si large peut représenter une difficulté pour les MSP, qui doivent prouver qu'ils comprennent et peuvent prendre en charge les nuances entre différents secteurs et les difficultés spécifiques rencontrées par les entreprises. Les MSP doivent donc offrir un large éventail de services aux clients pour répondre à leurs besoins. Par conséquent, ils doivent posséder des compétences et une expertise pointues dans divers domaines.

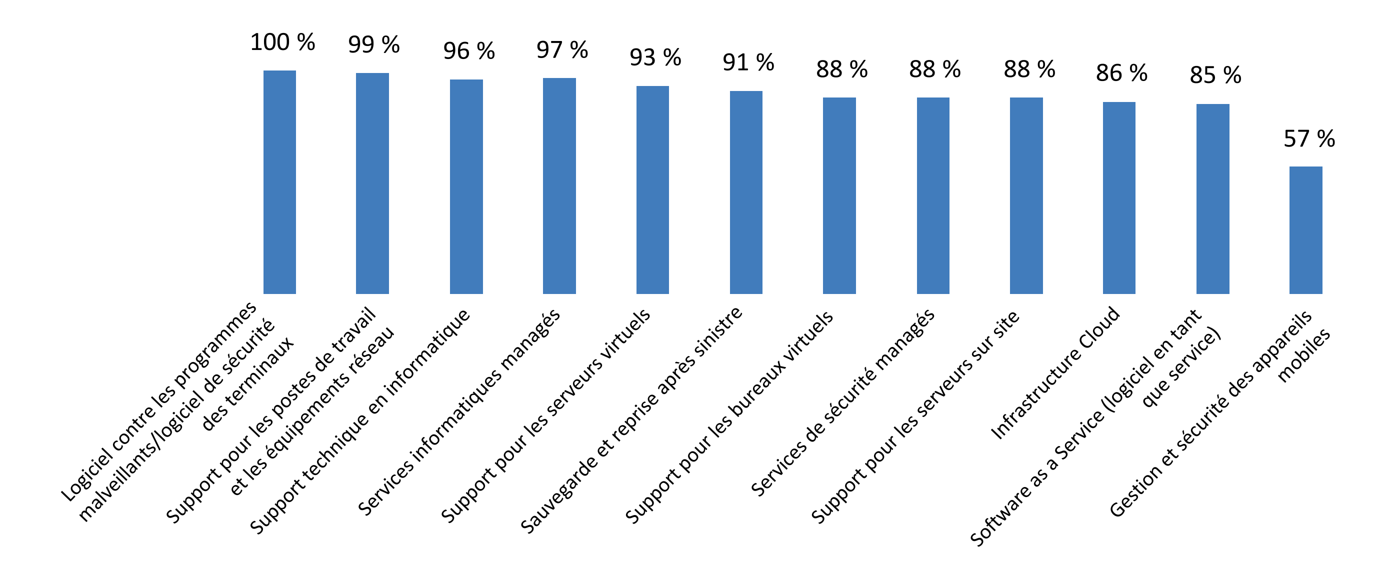


Figure 5. Aperçu des principaux « services managés » offerts aux clients

Toutefois, malgré le nombre élevé de clients, lorsque l'on étudie le nombre spécifique d'appareils que les MSP gèrent généralement, on découvre qu'un quart (23 %) d'entre eux s'occupent uniquement de 10 à 25 appareils par client. Pour 48 % des MSP, cela se réduit à moins de 10 « terminaux » par client.

Aspects positifs et négatifs

Une base de clients croissante peut être une arme à double tranchant pour les MSP. Bien que les entreprises réclament leurs services, c'est la concurrence accrue sur le marché qui rend les clients plus exigeants que jamais auprès de leur MSP. Cela est vrai pour les trois quarts (75 %) des MSP qui admettent que les exigences des clients et utilisateurs représentent un défi majeur. Le même nombre de MSP (78 %) considère également qu'il est difficile de trouver de nouveaux clients, les deux tiers (68 %) luttant pour maintenir leur rentabilité.

Le problème du chiffre d'affaires s'explique dans l'éventail des services que les MSP doivent fournir et les faibles niveaux de terminaux qu'ils gèrent effectivement par client. Pour renforcer leur valeur auprès des clients et pour créer des opportunités d'augmentation de leur chiffre d'affaires, les MSP pourraient offrir une réduction sur le logiciel de sécurité, afin de rendre le modèle externalisé plus rentable pour leurs clients et fidéliser ceux-ci sur le long terme.

La satisfaction de la clientèle étant au centre des priorités de nombreux MSP, il n'est pas surprenant de constater que les chiffres liés à la fidélisation sont la principale mesure de réussite pour 43 % des MSP, dont 41 % se fondent sur les sondages de satisfaction de la clientèle pour évaluer la performance de leur entreprise. En revanche, les mesures basées sur la valeur que les MSP offrent aux clients en matière de rentabilité (33 %) et d'efficacité (20 %) sont moins importantes.

Concernant les stratégies pour attirer les clients, la majorité (83 %) des MSP comptent sur le bouche à oreille ou les recommandations pour stimuler leur base de clients, la gestion de la réputation devenant ainsi un atout clé dans l'arsenal des MSP pour l'acquisition de nouveaux clients.

Malgré ces difficultés, les MSP dans toute l'Europe prévoient une forte croissance commerciale au cours des deux prochaines années et 63 % s'attendent à une croissance importante de leur chiffre d'affaires (jusqu'à 20 %). Cela reflète certainement la tendance actuelle sur le marché mondial et soutient le taux de croissance annuel prévu de 9,3 %.

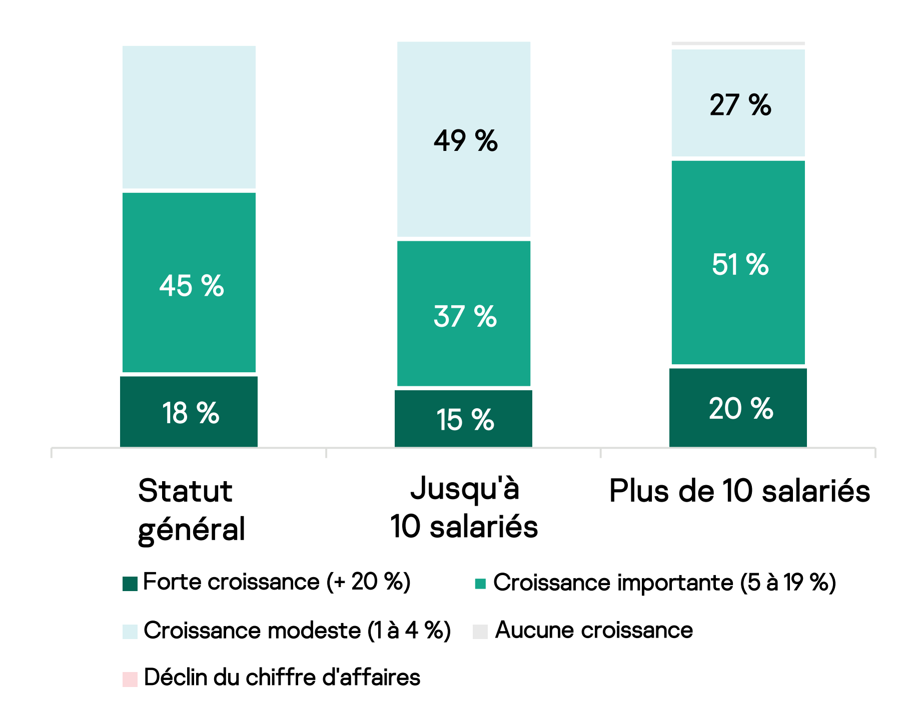


Figure 6. Croissance commerciale des MSP prévue

Le partenaire de sécurité idéal

Il est clair que l'externalisation de la gestion de la sécurité informatique occupe une place importante dans l'agenda des entreprises. Ainsi, comment les MSP peuvent-ils continuer à satisfaire ce besoin et à s'assurer que les services et les solutions qu'ils proposent sont à la hauteur des attentes de leurs clients ? Lorsqu'ils cherchent à établir un partenariat avec un fournisseur de solutions de sécurité informatique, 92 % des MSP prennent une décision en fonction de la réputation et du prix. Ces valeurs sont suivies de près par la facilité de gestion, d'intégration et d'achat de licence (88 %).

La façon dont les MSP achètent des licences a également une incidence sur le risque et la rémunération, contribuant à accélérer et à simplifier la prestation de services auprès de leurs clients. Les MSP préfèrent la flexibilité dans leurs licences, près de la moitié (47 %) ayant indiqué qu'ils préféraient acheter des licences individuelles pour chaque client. Parallèlement, les autres (44 %) choisissent de payer des logiciels et des services de sécurité informatique provenant de fournisseurs par l'intermédiaire d'un modèle d'abonnement mensuel. Ces deux options permettent aux MSP de se protéger dans le cas où un client changerait de partenaire. Ils peuvent également gérer plus efficacement leurs licences.

Les MSP préfèrent également bénéficier d'outils simples pour passer commande et gérer les licences. Ces points sont assez déterminants lorsqu'ils doivent choisir une fournisseur de solutions de sécurité. En fait, plus de la moitié d'entre eux (56 %) ont déclaré qu'ils utilisaient le portail de gestion des licences d'un fournisseur pour obtenir des licences. Les MSP bénéficient également des outils RMM (Remote Monitoring and Management) et PSA (Professional Service Automation) intégrés au logiciel de sécurité pour la surveillance et la gestion centralisées, ainsi que de l'automatisation des tâches de routine quotidiennes.

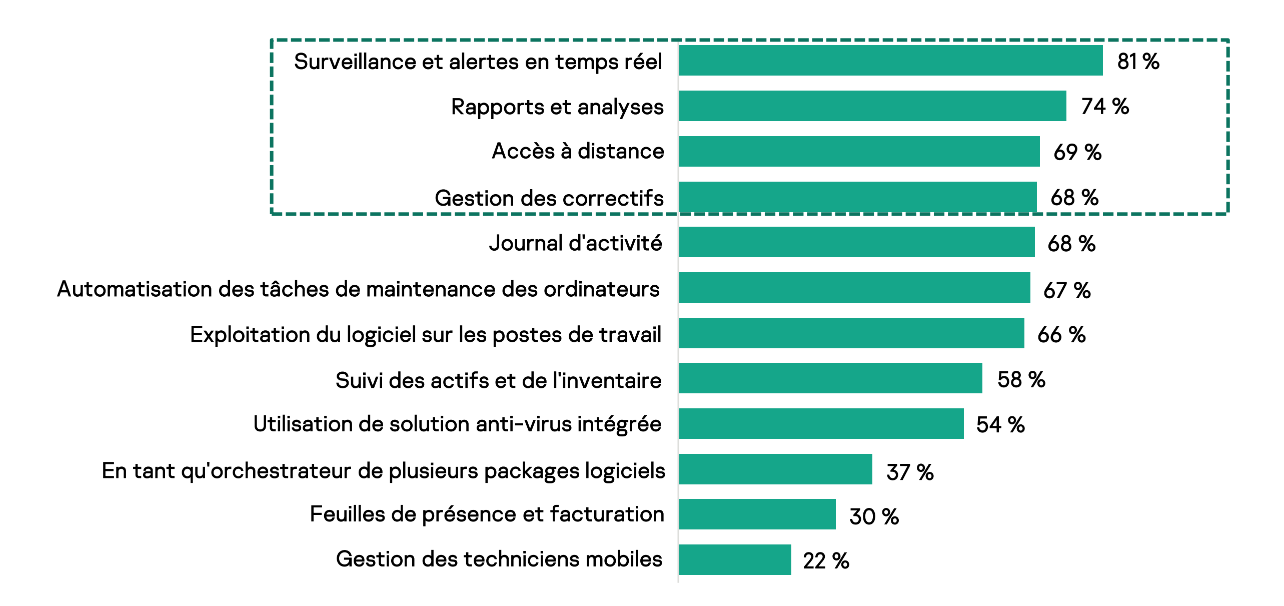


Figure 7. Principales utilisations de plateformes RMM parmi les MSP

Les hauts et les bas d'une relation

Qualités et difficultés

Comme dans n'importe quel type de relation, les deux parties s'attendent à en tirer le maximum, mais il existe inévitablement des difficultés et des obstacles à surmonter tout au long du parcours. Concernant les attentes des MSP actuels, le fait d'être un expert est la qualité que les clients recherchent en priorité (84 %), que ce soit pour des solutions sur site ou d'infrastructure Cloud. Les MSP doivent également être en mesure de satisfaire aux demandes de conformité et de règlementation (82 %), de réagir rapidement, ainsi que de respecter des accords de service exigeants (80 %).

Fait intéressant, les capacités en cybersécurité ont été particulièrement signalées comme étant un atout clé que les MSP doivent posséder, par près de trois quarts (74 %) des clients en quête de soutien de gestion informatique. Le fait que cette requête occupe une place si importante dans la liste des exigences est la preuve que les entreprises ont besoin d'un soutien supplémentaire pour suivre l'évolution du paysage de la cybersécurité.



Figure 8. Qualités les plus demandées par les clients auprès des MSP

En plus de ces exigences, on attend également des MSP qu'ils gèrent les imprévus. Malheureusement, être un fournisseur expert et fiable apporte de nouveaux défis à relever. Trois quarts (78 %) des clients s'attendent à ce que les MSP traitent des problèmes en dehors de leur contrat. Pour d'autres, les problèmes que les utilisateurs créent génèrent plus de travail pour eux (65 %) ou l'incapacité à suivre les processus du support technique (59 %) ajoute des tâches superflues à la liste de choses à faire.

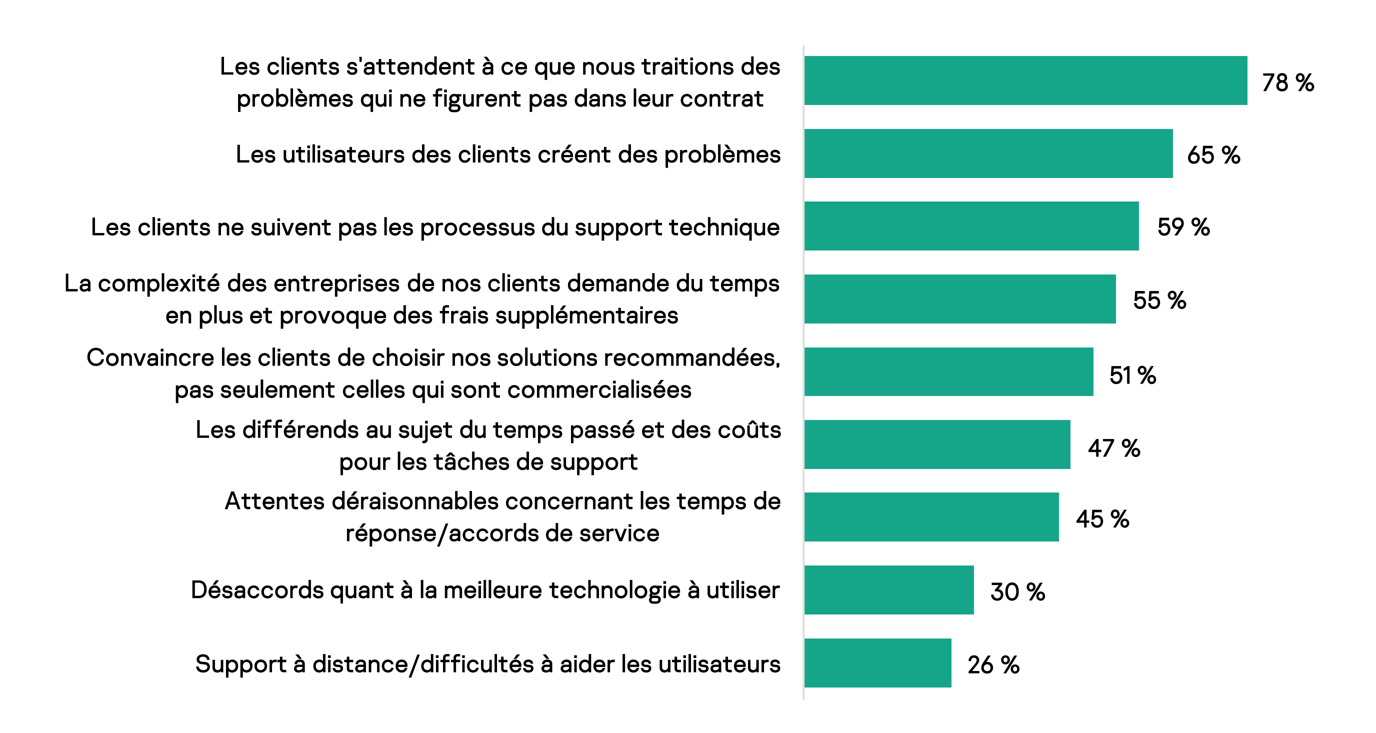


Figure 9. Problématiques rencontrées par les MSP avec leurs clients

Toutefois, la plus grande difficulté à laquelle les MSP sont confrontés est sans aucun doute le volume de cyberattaques et d'infections par un programme malveillant entraînant des interruptions d'activités pour leurs clients (72 %), suivi de près par les attaques de ransomware (65 %). Cependant, les menaces externes ne sont pas les seules à donner du fil à retordre aux MSP : le facteur humain entraîne toujours des problèmes, 69 % des MSP percevant les erreurs d'utilisateur et le non-respect des politiques de sécurité comme les principales menaces pour la sécurité du client.

Ce que cela signifie pour les MSP

L'impact de tout incident de sécurité peut avoir de lourdes conséquences, non seulement pour le client, mais aussi pour le MSP impliqué. La récente violation de données de Capital One, qui a touché plus de 100 millions de personnes, était due à un « pare-feu d'application Web mal configuré sur Amazon Web Services ». AWS était dans la ligne de mire, mais n'a pas été piraté. Le problème a été imputé à un client qui n'avait pas correctement configuré le pare-feu du Cloud.

Ce n'est qu'un exemple de cas où une tierce partie peut être dans la ligne de tir pour une violation de données de client et ce ne sera certainement pas le dernier. En fait, parmi les clients de MSP sondés qui ont subi une violation de données, 43 % ont rejeté la responsabilité sur leur MSP, et seulement 41 % ont reconnu que leur propre personnel était en faute. Fait plus surprenant, un quart (27 %) de ceux qui ont expérimenté une violation l'ont imputée à un manque de connaissances en matière de sécurité informatique de la part de leur fournisseur de services.

Toutefois, les erreurs de sécurité du client peuvent également avoir un impact sur les MSP en termes de temps passé à résoudre le problème (67 % d'accord), dont un tiers (38 %) ont même perdu de l'argent en traitant le problème qui n'était pas dû à leur négligence ou à leur manque d'expertise.

Conclusion et recommandations

Il est clair que la réduction des coûts et le fait de tirer le meilleur parti des budgets informatiques disponibles est le principal facteur pour que les entreprises externalisent leur gestion informatique. En plus du manque de ressources et de compétences internes en sécurité informatique, il existe une opportunité évidente pour que les MSP deviennent des experts en cybersécurité et comblent des lacunes relatives à la gestion de la sécurité pour les entreprises dans toute l'Europe.

Il est donc essentiel que les MSP soient entièrement équipés pour offrir ce niveau de service et répondre à la demande croissante en services de sécurité externalisés. Afin d'attirer de nouveaux clients et d'augmenter leur chiffre d'affaires, ils doivent élargir la liste des services qu'ils proposent, ainsi que se concentrer sur leur positionnement sur le marché et la gestion de leur réputation pour se démarquer de leurs concurrents.

Les clients s'attendent à une protection, mais aussi à une expertise en sécurité de la part de leur MSP. Un manque de compétence dans ce domaine peut conduire à perdre des clients et à échouer à établir le rapport de confiance qu'ils recherchent. Il est impératif pour les MSP d'établir des rapports de confiance et une fidélité avec les clients, ce qui peut être fait seulement s'ils disposent des outils et des compétences appropriés afin d'accompagner les clients à chaque étape du processus.

La réputation est un facteur clé pour attirer et fidéliser les clients. Un seul faux pas peut avoir des effets durables et désastreux. Disposer d'une large gamme de services de sécurité, soutenue par un partenaire en cybersécurité solide et fiable, favorisera les MSP pour réaliser la croissance du marché prévue, entraînant des bénéfices et une stabilité à long terme des activités.

Les fournisseurs ont un grand rôle à jouer et peuvent offrir un soutien essentiel aux MSP. Ce n'est un secret pour personne : les MSP chercheront à étendre leurs services de sécurité durant les prochaines années. Par conséquent, les fournisseurs qui peuvent offrir des évaluations de sécurité, une réponse aux incidents et des passerelles de messagerie ou Web devraient bénéficier d'une hausse de la demande.

Les fournisseurs de solutions de sécurité peuvent transmettre une expertise importante en cybersécurité et renforcer les compétences, ainsi que soutenir les ventes. Le programme MSP de Kaspersky offre des produits de cybersécurité dédiés à l'utilisation des MSP, avec des formations, de la documentation pédagogique et des événements spécifiques au marché de la cybersécurité. Kaspersky possède un vaste portefeuille conçu pour les MSP, qui leur permet de déployer des solutions sur site ou basées dans le Cloud, depuis la protection des terminaux jusqu'à la sécurité des Cloud hybrides, en passant par la protection de la messagerie et de l'accès au Web. Ces solutions peuvent être intégrées aux plateformes RMM (Remote Monitoring and Management) et PSA (Professional Service Automation), afin d'aider les fournisseurs de services à automatiser les tâches de routine. Le programme partenaires comprend également des avantages commerciaux et financiers pour tous les partenaires Kaspersky.

Plus d'informations sur le programme MSP de Kaspersky sont disponibles sur le site Web de Kaspersky.